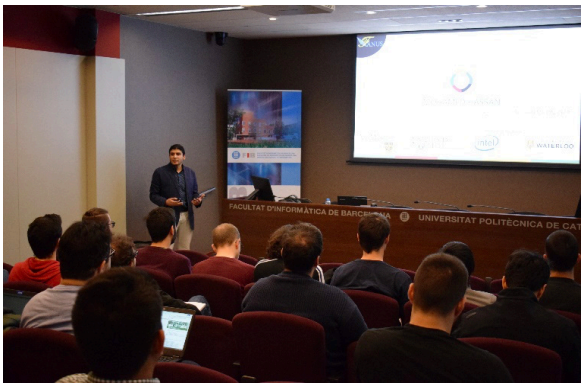
February 18th, 2020

Towards Predictable, Secure, and Verified Cyber-Physical Systems-on-Chip

Dr. Mohamed Hassan
Assistant Professor at McMaster University, Canada

Abstract

The unleashed Cyber-Physical Systems (CPS) and Internet of Things (IoT) revolution creates exceptional opportunities in many domains such as healthcare, smart power grid, automotive, industrial robots, and transportation systems. Systems-on-Chip (SoCs) present appealing platforms that enable this revolution due to their performance, power, and area (PPA) advantages in addition to their heterogeneity, leading to Cyber-Physical Systems-on-Chip (CPSoCs). However, CPSoCs are not possible without addressing the one big concern associated with the prevalence of CPS: safety. Safe CPSoCs must be predictable, secure and verifiable. 1) Predictability ensures the satisfaction of timing requirements. Unpredictable CPSoCs can fail to meet timing deadlines, which leads to severe consequences such as life losses (think in the air bag in your car). However, current commodity SoCs are not predictable. They adopt numerous architectural optimizations that offer high-performance at the cost of huge variability in timing. 2) Security is one of the biggest challenges facing architects of CPS. Unlike traditional



computing systems, CPS manage sensitive tasks; therefore, any security breach could lead to catastrophic consequences. These consequences range from revealing personal information (e.g., from wearable devices) to a global threat (e.g., compromising a nuclear plant). Consequently, ensuring the security of CPSoCs is a first-class mission. 3) Verifiability, reliability and correct functionality in CPSoCs are of a vital importance. Think for example in self-driving cars, self-adaptive home appliances, or smart power grids. Similar to untimeliness, malfunctioning in these systems can also lead to life losses. Accordingly, the rigorous verification of each system component is unavoidable process for these markets to successfully scale.

In this talk, I present several novel solutions to provide predictable, secure, and verified CPSoCs. Finally, I highlight research directions towards enabling the widespread of CPSoCs and open problems yet to be addressed.

Short bio

Dr. Mohamed Hassan is currently an Assistant Professor at McMaster University, Canada, where he leads the Fanus research lab focusing on intelligent Cyber-Physical Systems-on-Chip. Before joining McMasterU, he was an Assistant Professor at University of Guelph, Canada. He also worked as a System-on-Chip (SoC) R&D lead engineer at Intel. He obtained his PhD from University of Waterloo in 2017, where he was a member of the Computer Architecture and Embedded Systems Research (CAESR) lab. Dr. Hassan won multiple awards including the Discovery Launch Supplement Award from NSERC, the PhD Thesis Award and the Faculty of Engineering (FOE) Award from University of Waterloo, the Best Paper Award in ACM/IEEE Embedded Systems Week, and the Best Paper Award from the IEEE Real-Time Systems Symposium.